## REMARKS

This is a Response to Final Office Action accompanying a Request for Continued Examination. Claims 1-39 are pending in the present application. Claims 1-2, 14-15, and 27-28 were amended; no claims were added. Support for amendments to the claims may be found in the specification at least on pages 15-16, 19, and 31-32, and Figure 4. Reconsideration of the claims is respectfully requested.

## I. Supplemental Information Disclosure Statement

A Supplemental Information Disclosure Statement is included with this submission. The Supplemental IDS includes the following additional information: The present application is related to issued patent titled "System and Method for Multiple Virtual Private Network Authentication Schemes," US Patent No. 6,938,155, filed May 24, 2001; co-pending published application "System and Method for Dynamically Determining CRL Locations and Access Methods," Publication No. 2002/0178361, filed May 24, 2001; and co-pending published application "System and Method for Selectively Confirming Digital Certificates in a Virtual Private Network," Publication No. 2002/0178240, filed May 24, 2001.

## II. 35 U.S.C. § 102, Anticipation: Claims 1, 5-14, 18-27, and 31-39

The examiner has rejected claims 1, 5-14, 18-27, and 31-39 under 35 U.S.C. § 102(e) as being anticipated by *D'Sa* et al., System and Method for Multiple Virtual Private Network Authentication Schemes, U.S. Patent Publication No. 2002/0178355, November 28, 2002, now US Patent No. 6,938,155 (hereinafter "*D'Sa*"). This rejection is respectfully traversed.

The examiner states on page 2 of the Office Action dated August 23, 2005 that:

> As per claims 1, 14, and 27, the applicant describes a data processing system for defining a configuration of IP security tunnels comprising the following limitations which are met by D'Sa:
>
> a) a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types ([0041],[0O47]-[0048],Fig 2);
>
> b) said system for automatically configuring an IP security tunnel utilizing said security policy 25 specification format ([0042],[0047]-[0048],Fig 2);

Office Action dated August 23, 2005, page 2.

*D'Sa* fails to teach or suggest selecting "a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy specification format," as is recited in amended independent claims 1, 14, and 27. Independent amended claim 1, which is representative of other rejected independent claims 14 and 27, recites as follows:

> 1. A method in a data processing system for automatically configuring IP security tunnels, said method comprising the steps of:
>
> exchanging identification data with a remote computer system;
>
> determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system;
>
> selecting a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent; and
>
> defining a configuration of an IP security tunnel utilizing said security policy specification format.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 194). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983).

*D'Sa* does not teach each and every feature of the claims arranged as they are in the claims. Specifically, *D'Sa* does not teach automatically configuring IP security tunnels by "selecting a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent; and defining a configuration of an IP security tunnel utilizing said security policy specification format," as is recited in claim 1.

*D'Sa* does not teach or disclose "selecting a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine

types," as is recited in claim 1. The Examiner alleges this feature is taught by *D'Sa* at [0041], [0047]-[0048], and Figure 2.

**Figure 2** of *D'Sa* is shown as follows:

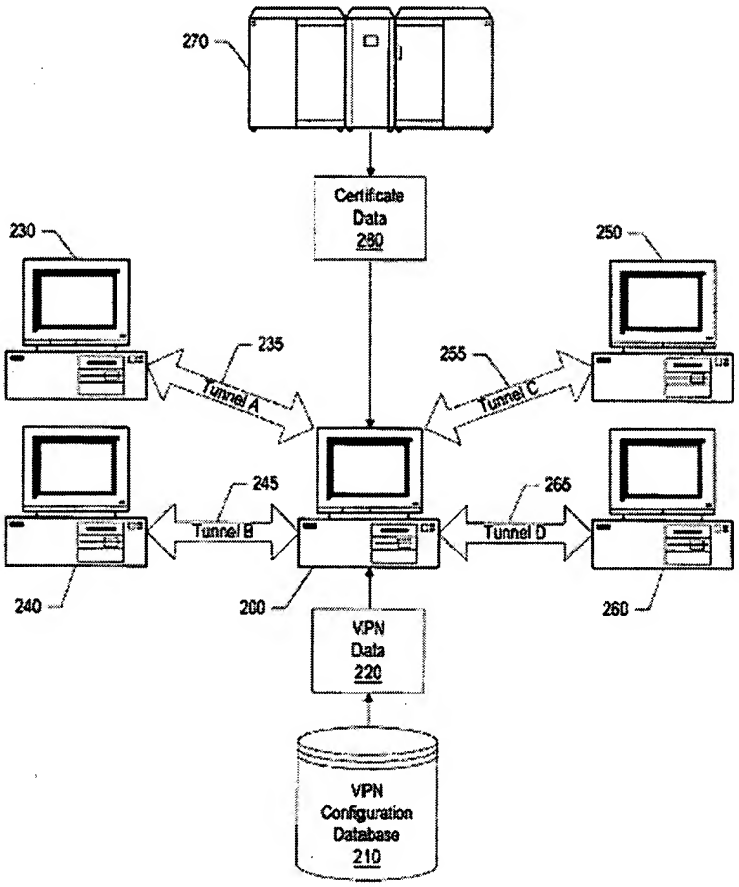



***Figure 2***

As can be seen, **Figure 2** does not show the selecting step of claim 1 much less a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types. This figure shows tunnels connecting multiple computers. The figure does not teach or disclose "**selecting a security policy specification format" for defining a configuration of a tunnel,** as is claimed in independent claim 1. Nowhere is a security policy specification format shown, much less one that is capable of being utilized by a plurality of different operating systems and a plurality of different machine types. Nor is anything shown in Figure 2 to teach or disclose the selecting step using this security policy specification format.

Next, *D'Sa* teaches as follows:

> FIG. 2 shows a diagram of tunnels being created between a computer and other computers using VPN configuration data and certificate data. Computer system 200 establishes various tunnels used to securely transmit data to and from other computer systems. Computer systems that computer system 200 wishes to securely communicate with over a VPN are identified in VPN configuration database 210. VPN data 220 contains information for connecting with a particular computer system. Using VPN configuration database 210, any number of VPNs can be established between computer system 200 and other computer systems. Some VPNs use certificate data 280 supplied by a trusted third party computer system 270. The use of a trusted third party aids in authenticating users and ensuring that an impostor does not take the place of another computer system.
>
> In the example shown, computer system 200 establishes tunnel A 235 securely connecting first computer system 230 with computer system 200. Likewise, tunnel B 245 securely connects second computer system 240 with computer system 200, tunnel C 255 securely connects third computer system 250 with computer system 200, and tunnel D 265 securely connects fourth computer system 260 with computer system 200. Each of these computer systems, 230, 240, 250, and 260, have identification information and authentication information stored in VPN configuration database 210.

*D'Sa*, [0040] and [0041].

Here, *D'Sa* teaches that **tunnels are being created** between computer systems **using preexisting configuration data** present in a VPN configuration database. *D'Sa* discloses utilization of the information contained in the configuration database to establish VPNs for transmission of data between the computer systems identified in the database. However, *D'Sa* does not teach selecting "a security policy specification format" that is used to **define a configuration of a tunnel**, as is claimed in claim 1. To the contrary, *D'Sa* teaches configuration database containing pre-existing configurations for a tunnel between a remote computer and a local computer. Establishing a format for defining a configuration of a security tunnel when a preexisting tunnel does not already exist in a configuration database is not taught in the cited portions of the reference. Thus, *D'Sa* does not teach or disclose selecting "a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent," as recited in claim 1.

*D'Sa* does not teach or suggest "defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy

specification format," as is recited in amended claim 1. The Examiner believes that this feature is taught in Figure 2. Figure 2 discloses that security tunnels are present between computers, but in no way provides any teaching or disclosure for defining a configuration of an IP security tunnel utilizing said security policy specification format.

The examiner believes that the defining step is taught in the following section of *D'Sa*:

> FIG. 3 shows a database diagram of tables used in configuring tunnels between the computer and other computer systems. VPN configuration database 300 is shown with four tables. Endpoints table 310 includes a list of configured tunnels between the computer system and other computer systems. One end of each endpoint identifies the computer system, while the other end of the endpoint identifies a remote computer. Each of the computers included in endpoints table 310 is identified with an identifier, such as an address. In addition, endpoints table 310 includes IP addresses for the remote computer systems. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example 1.160.10.240 could be an IP address. Within an isolated network, IP addresses can be assigned at random so long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates. The four numbers in an IP address are used in different ways to identify a particular network and a host on that network. Finally, endpoints table 310 includes a flag indicating whether a Certificate Revocation List (CRL) is used to check whether a given certificate has been revoked. Other valid ID types include FQDN, user@FQDN, distinguished names, and key IDs.

*D'Sa*, [0042].

As can be seen, this cited portion of *D'Sa* discloses a configuration database containing a list of configured tunnels between a computer system and a remote computer system to determine a compatible authentication system. Although *D'Sa* appears to teach use of information in a configuration database for selecting an access method for computer systems requesting a VPN, this section of *D'Sa* does not teach automatically configuring a security tunnel or utilizing a standardized security policy format capable of being used by a plurality of different operating systems as recited in claim 1.

*D'Sa* teaches:

> It has been discovered that a configuration tool can be provided to allow a computer system to be a member of multiple virtual private networks (VPSs). A

> database is included to store information about the various tunnels that can be used from the local computer system. An endpoints table includes a list of the configured tunnels. This list includes local-remote pair data with identifying information for each machine. A policy table is used to determine which access method(s) are used to connect the local computer system to the remote computer system. In addition, a preference order is provided in order to use multiple access methods in a preferred order. Two additional table include key information regarding the connection between the local and remote computer systems. A pre-shared keys table includes pre-shared key information, while a digital certificate table includes public key information and other digital certificate information.

*D'Sa,* [0021].

As shown above, *D'Sa* teaches selection of an access method by utilizing information in a configuration database regarding various tunnels that can be used by the computer systems requesting a VPN, including a list of already configured tunnels, a preference order for access methods where multiple access methods are available and connection information for the remote computer system. *D'Sa* does not teach or suggest a standardized format utilized in configuring IP security tunnels. Thus, *D'Sa* does not teach or disclose "defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy specification format," as in claim 1.

Therefore, *D'Sa* fails to teach each and every feature recited in claim 1. Other independent claims 14 and 27, which recite subject matter addressed above with regard to claim 1, are distinguishable over *D'Sa* based on the same rationale set forth above with regard to claim 1. In addition, independent claim 14 recites additional features not suggested by the reference. Amended claim 14 recites "a computer usable medium having computer usable program code for defining a configuration of IP security tunnels." As discussed above, *D'Sa* merely teaches selection of an access method by utilizing information in a configuration database regarding various tunnels that can be used by a computer system requesting a VPN. The cited portions of *D'Sa* do not teach or disclose "defining a configuration of IP security tunnels," as is claimed in independent claim 14. Therefore, *D'Sa* does not teach each and every feature of independent claim 14.

By virtue of their dependency on independent claims 1, 14, and 27, *D'Sa* does not teach each and every feature of dependent claims 5-13, 18-26, and 31 -39. Additionally, claims 5-3, 18-26, and 31-39 claim other additional combinations of features not suggested by the reference.

For example, with respect to claims 6, 11, 16, 24, 29, and 37, the Examiner alleges that *D'Sa* discloses a protection element at paragraph [0099], which states as follows:

> Depending on the authentication method used, key values are fetched from Public/Private Keys database 740 and Pre-Shared Keys database 745. For authentication methods that use public key encryption, Public/Private Keys database 740 is used. The Public/Private Keys database includes local private keys and corresponding digital certificates which contain the corresponding public key of the local ID and signing certificates including public keys corresponding to the signing certificates.

*D'Sa*, [0099].

In a VPN, computer systems can use pre-shared key encryption and a combination of private key, which is known only to the user's computer, and public key, which is given by the user's computer to any other computer that wants to communicate securely with it. *See D'Sa,* paragraph [0011]-[0012]. This section of *D'Sa* discloses fetching key values from a Public/Private Keys database and a Pre-Shared Keys database for authentication. However, there is nothing in this, or any other section of *D'Sa*, that teaches "a protection element in said security policy specification format, said protection element including a listing of IKE transforms," as is recited in claims 6, 11, 16, 24, 29, and 37.

As to claims 11, 24, and 37 the Examiner alleges that *D'Sa* teaches an IPsec proposal element, an IPsec authentication header element, and an IPsec protection element at paragraphs [0071], [0072], and [0146], which are as follows:

> Initiator Proposal List Index—an index to a initiator proposal list record (see Proposal List 725, below). If the Initiator Proposal List Index is null then initiation with the remote ID is not allowed (i.e., the system only acts as a responder to the remote ID).
>
> Responder Proposal List Index—an index to a responder proposal list record (see Proposal List 725, below). If this value is null, then response is not allowed (i.e., system only acts as an initiator when dealing with the remote ID). If both the Initiator Proposal List Index and the Responder Proposal List Index values are null, then no negotiation is allowed between the systems.

*D'Sa*, [0071]-[0072].

> The number authentication header (AH) Transforms, if this value is 0 then AH will not be proposed.

*D'Sa*, [0146].

Here, *D'Sa* discloses an Initiator Proposal List Index and a Responder Proposal List Index regarding the method of *D'Sa* by which an initiating computer proposes one or more authentication methods and a responder computer selects an authentication method from the initiator's proposal list. The above cited portions of *D'Sa* does not disclose any teachings regarding the Internet Protocol Security Protocol (IPsec) or "an IPsec proposal element, an IPsec ESP protocol element, an IPsec authentication header element, and an IPsec protection element" in a security policy specification format, as is claimed in claims 11, 24 and 37.

In regards to claims 12-13, 25-26, and 38-39, the Examiner states that *D'Sa* describes the step of automatically configuring an IP security tunnel utilizing the security policy specification format at *D'Sa*, paragraphs [0040] and [0041], which are set forth above. Here, *D'Sa* discloses establishing a VPN between a computer system and remote computer systems by using a configuration database containing identification data and authentication information for the computer system and the remote computer systems. However, *D'Sa* does not disclose a standardized format or "automatically configuring an IP security tunnel utilizing said security policy specification format," as is recited in claims 12, 15, and 38. Consequently, it is respectfully urged that the rejection of claims 1, 5-14, 18-27, and 31-39 have been overcome.

Therefore, the rejection of claims 1, 5-14, 18-27 and 31-39 under 35 U.S.C. § 102 has been overcome.

Furthermore, *D'Sa* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *D'Sa* actually teaches away from the presently claimed invention because it teaches utilization of a list of already configured tunnels in the Endpoints table of the configuration database and preference data for use in determining a compatible access policy as opposed to automatically configuring an IP security tunnel by establishing a security policy specification format capable of being utilized by a plurality of different operating systems and defining a configuration of an IP security tunnel utilizing the security policy specification format, as in the presently claimed invention. Absent the Examiner pointing out some teaching or incentive to implement *D'Sa* and automatically configuring IP security tunnels by establishing a security policy specification format for defining a configuration of an IP security tunnel, one of ordinary skill in the art would not be led to modify *D'Sa* to reach the present invention when the reference is examined as a whole. Absent some teaching,

suggestion, or incentive to modify *D'Sa* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, the rejection of claims 1, 5-14, 18-27, and 31-39 under 35 U.S.C. § 102(e) has been overcome.

## III. 35 U.S.C. § 102, Anticipation: Claims 1, 14, and 27

The examiner has rejected claims 1, 14, and 27 under 35 U.S.C. § 102(e) as being anticipated by *Bendinelli* et al., Methods and Systems for Enabling a Tunnel Between Two Computers on a Network, U.S. Patent No. 6,631,416, October 7, 2003 (hereinafter "*Bendinelli*"). This rejection is respectfully traversed.

The examiner states on pages 3-4 of the Office Action dated August 23, 2005 that:

> As per claims 1, 14, and 27, the applicant describes a data processing system for defining a 25 configuration of IP security tunnels with the following limitations which are met by Bendinelli:
>
> a) a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types (Col 17, lines 36-63);
>
> b) said system for automatically configuring an IP security tunnel utilizing said security policy specification format (Col 11, lines 36-63);

Office Action dated August 23, 2005, pages 3-4.

*Bendinelli* does not teach or disclose automatically configuring IP security tunnels by "selecting a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent" and "defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy specification format," as is recited in amended independent claims 1, 14, and 27. The Examiner alleges that these features are taught by *Bendinelli* at column 17, lines 36-63, which is as follows:

> FIG. 3 shows an exemplary flowchart for initially registering one or more gateways with the control system 175. Referring to FIGS. 1 and 3, the user may register at least one of the gateways 150-153 with the control system 175 (step 310) and define a configuration for the registered gateways 150-153 (step 320). In one embodiment, the user may contact the control system 175 through the Internet using a web browser to specify a particular configuration for a gateway. This

specified configuration information may include a name for the gateway and a name for the virtual private network. This name for the virtual private network will hereinafter be referred to as the virtual private network's domain name.

The control system 175 may use the specified configuration to assemble code and information, such as program code and textual information (e.g., Extensible Markup Language also referred to as "XML"), in the form of a disk image (step 330). This disk image may include all the program code and information needed to configure gateways 150-153 for establishing one or more virtual private networks established over communication channel 120. The disk image may then be provided to the user and installed on a processor, such as a personal computer or a general-purpose computer (step 340). When the processor reboots, it uses the information provided in the disk image to configure itself as a gateway capable of establishing secure tunnels to the control system 175.

*Bendinelli*, column 17, lines 36-63.

Here, *Bendinelli* discloses the process whereby a user initially registers with a control system to participate in a VPN. According to *Bendinelli*, a user may contact a control system and provide configuration information to the control center, such as a name for the gateway and a name for the VPN, which is referred to by *Bendinelli* as a VPN domain name. The control system then provides a program code containing information and code needed to configure a gateway for establishing a VPN. The program code, once installed, enables configuration of a gateway. However, the cited portion of *Bendinelli* does not teach or disclose a security policy specification format capable of being used by a plurality of different operating systems and different machine types. Nor does *Bendinelli* teach or suggest a security policy format for defining a configuration of a security tunnel. In fact, *Bendinelli* does not even mention a security policy anywhere in this cited portion of the reference. To the contrary, *Bendenilli* teaches a user requesting a VPN, answering some questions regarding the desired VPN and receiving a program code to establish the VPN. *Bendinelli* teaches:

[A] prospective user or customer may contact a mediation point or a control system, such as a network operations center via a base network, such as the Internet, and indicate a desire to establish one or more virtual private networks. After answering a series of questions posed by the network operations center, the user receives program code and information for loading onto one or more processors, such as personal computers. The program code and information may be in the form of a disk, such as an optical disk or floppy disk, downloaded over the Internet and onto a disk, or installed directly over the Internet on to a computer. The program code may be distributed to other computers at other desired sites user sites as well. Alternatively, the program code and information

may be preinstalled on a computer and delivered to the user.

The user then runs or boots a computer with the provided code and information. When the computer is booted, it thereafter communicates with the network operations center over the Internet to receive further information such that the computer is configured as a gateway or a computer capable of participating in one or more virtual private networks enabled by the network operations center over a base network, such as the Internet.

*Bendinelli*, column 10, line 61-column 12, line 16.

As is shown above, *Bendinelli* does not describe automatic configuration of a security tunnel utilizing a standardized security policy format. According to the teachings of *Bendinelli*, a user requests establishment of a VPN, user provides information regarding the VPN requested, and control system sends user **a disk containing information and program code for configuring a tunnel**. *Bendinelli* merely provides a configuration for a tunnel rather than a specification format for defining a configuration for a tunnel. In contradistinction, the present invention in claim 1 claims **"selecting a security policy specification format" for defining a configuration of an IP security tunnel** if a predefined security policy is absent. Thus, *Bendinelli* fails to teach or suggest "selecting a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent; and defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy specification format," as claimed in claim 1.

Moreover, *Bendenilli* fails to teach "exchanging identification data with a remote computer system" and "determining whether a predefined security policy exists corresponding to the remote computer system," as is now recited in amended independent claim 1. *Bendinelli* does not teach, disclose or suggest exchanging identification data with a remote computer. As discussed above, *Bendinelli* merely teaches a user requests a VPN from a control center, user provides information regarding the requested VPN, and control center sends program code to user to configure a VPN. A data processing system "exchanging identification data with a remote computer system" is not taught or disclosed.

Furthermore, *Bendinelli* fails to teach or disclose determining whether a predefined security policy exists based on the identification data and establishing a security policy specification format in response to determining a predefined security policy does not exist.

*Bendenilli* merely teaches provision of program code for configuring a VPN in response to user request for a specified VPN. *Bendenilli* does not teach or disclose a security policy of any kind. Therefore, *Bendinelli* does not teach each and every feature of independent claim 1.

Independent amended claims 14 and 27 recite similar subject matter addressed above with respect to claim 1. Therefore claims 14 and 27 are distinguishable over *Bendinelli* under the same rationale as discussed above with regard to claim 1. Therefore, the rejection of claims 1, 14 and 27 under 35 U.S.C. § 102 has been overcome.

Furthermore, *Bendinelli* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Bendinelli* actually teaches away from the presently claimed invention because it teaches a user registering with a control system to request a VPN as opposed to selecting a standardized security policy specification format capable of configuring an IP security tunnel on a plurality of different operating systems and a plurality of different machine types, as in the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement *Bendinelli* and automatically configuring an IP security tunnel utilizing a security policy specification format, one of ordinary skill in the art would not be led to modify *Bendinelli* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Bendinelli* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, the rejection of claims 1, 14, and 27 under 35 U.S.C. § 102(e) has been overcome.

## IV. 35 U.S.C. § 103, Obviousness: Claims 2-4, 15-17, and 28-30

The examiner has rejected claims 2-4, 15-17, and 28-30 under 35 U.S.C. § 103(a) as being unpatentable over *Bendinelli* in view of Pfeiffer (Pfeiffer, Ralph I. March 2, 1999. XML Tutorials for Programmers. retrieved from http://www.informatik.hu-berlin.de/~xing/Lib/RIP-writing.pfg) (hereinafter "*Pfeiffer*"). This rejection is respectfully traversed.

The examiner states on page 4 of the Office Action dated August 23, 2005 that:

> As per claims 2-4,15-1 7, and 28-30, the applicant describes the system of claims 1,14, and 27, which are met by Bendinelli (see above),

with the following limitation which is met by Bendinelli in view of Pfeiffer:

Further comprising said security policy specification format being established as a DTD file (Bendinelli: Col 17, lines 36-63; Pfeiffer: pages 5-6);

Bendinelli discloses all the limitations of independent claims 1,14, and 27. However, Bendinelli discloses that the security policy specification format is established as an XML file, not a DTD file. Pfeiffer discloses that a DTD file commonly stores policy and rules. Combining Pfeiffer with Bendinelli would allow the security policy specification format to be stored in a DTD file instead of an XML file. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Pfeiffer with those of Bendinelli because a DTD file is another means to store a security policy specification format and DTD files typically store policy and rules.

Office Action dated August 23, 2005, page 4.

**A. The Examiner bears the burden of establishing a *prima facie* case of obviousness.**

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). In this case, the examiner has failed to establish a *prima facie* case of obviousness because the cited references do not teach or suggest the features of the present invention as believed by the examiner and the references cannot be properly modified or combined to reach the presently claimed invention for the reasons stated below.

**B. All claim limitations must be considered, especially when missing from the prior art.**

Additionally, in comparing Reference to the claimed invention, the claim limitations of the presently claimed invention may not be ignored in an obviousness determination. Claims 2-4, 15-17, and 28-30 are dependent on independent claims 1, 14, and 27. As shown above, each and every feature of the independent claims are not show in *Bendinelli.* Thus, at least by virtue of their dependency, dependent claims 2-4, 15-17, and 28-30 are distinguishable over *Bendinelli* for the same reasons set forth above with regard to independent claims 1, 14, and 27. Moreover, these claims recite additional combinations of features not taught, disclosed or suggested by the cited references. Dependent claim 2, which is representative of other rejected dependent claims 3-4, 16-17, and 28-30, with respect to similarly recited subject matter, recites as follows:

2. The method according to claim 1, further comprising:
establishing a security policy specification format capable of being utilized

by a plurality of different operating systems and a plurality of different machine types; and

establishing said security policy specification format as a DTD file.

As discussed above, *Bendinilli* does not teach or suggest a security policy specification format capable of being utilizing by a plurality of different operating systems and a plurality of different machine types. Nor does *Bendinelli* teach or suggest the establishing step claimed in amended claim 2.

Moreover, the Examiner admits that *Bendinelli* does not disclose the use of a DTD file, but states that *Bendinelli* discloses a security policy specification format is established as an XML file at column 17, lines 36-63, which is quoted above. As discussed above, *Bendinelli* merely discloses the process whereby a user initially registers with a control system to participate in a VPN. According to *Bendinelli*, a user may contact a control system and provide configuration information to the control center, such as a name for the gateway and a name for the VPN, which is referred to by *Bendinelli* as a VPN domain name. Although *Bendinelli* describes a user providing configuration information, such as a name for a gateway and a name for the VPN, and control system providing a program code that may be in provided in XML, Bendinelli does not teach or suggest establishing a security policy specification format or the security policy format as a DTD file. In fact, the cited portion of the reference does not even mention a DTD file or a security policy. Therefore, *Bendinelli* fails to teach or suggest "establishing said security policy specification format as a DTD file," as is recited in dependent claims 2, 15, and 28.

Moreover, *Pfeiffer* fails to make up for the deficiencies of *Bendinelli.* The Examiner recognizes that *Bendinelli* does not disclose a DTD file but believes *Pfieffer* discloses a DTD file commonly stores policy and rules. However, even if *Pfeiffer* could teach that a DTD file can be used to store policy and rules, such teaching are insufficient to teach or suggest establishing a security policy specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types; and defining a configuration of an IP security tunnel utilizing said security policy specification format.

Moreover, *Pfeiffer* fails to teach or suggest "exchanging identification data with a remote computer system; determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system" and selecting a security policy

specification format capable of being utilized by a plurality of different operating systems and a plurality of different machine types if a predefined security policy is absent;" and defining a configuration of an IP security tunnel between the data processing system and the remote computer system utilizing said security policy specification format," as is now recited in amended independent claim 1. Therefore, *Pfeiffer* fails to make up for the deficiencies of *Bendinelli*. Thus, the references cannot be combined to produce the claimed invention.

**C. The proposed modification would not be made when *Bendinelli* is considered as a whole.**

The proposed combination of *Bendinelli* and *Pfieffer* would not be made when *Bendinelli* is considered as a whole. "It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. 685, 687 (Fed. Cir. 1986). When *Bendinelli* is examined as a whole, *Bendinelli* teaches one of ordinary skill in the art that program code provided to a user may be provided to a user as, for example, Extensible Markup Language (XML), in the form of a disk. Therefore, when *Bendinelli* is considered as a whole, the sole purpose taught or suggested for XML is as a possible form of program code and information provided to user on a disk to establish a VPN.

When *Pfieffer* is examined as a whole, *Pfieffer* teaches one of ordinary skill in the art that a DTD file is a grammar that describes what tags and attributes are valid in an XML document. *Pfeiffer* does not teach or address the problem of establishing a security policy or configuring a security tunnel in a virtual private network. Thus, *Bendinelli* and *Pfieffer,* when considered as a whole, fail to teach or suggest establishing a security policy specification format as a DTD file for the purpose of defining a configuration of an IP security tunnel, as in claim 2. Therefore, the proposed combination of the references would not be made when the references are considered as a whole.

**D. Stating that it is obvious to try or make a modification or combination without a suggestion in the prior art is not *prima facie* obviousness.**

The mere fact that a prior art reference can be readily modified does not make the modification obvious unless the prior art suggested the desirability of the modification. *In re*

*Laskowski*, 871 F.2d 115, 10 U.S.P.Q.2d 1397 (Fed. Cir 1989); *see also In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992); *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1993). The Examiner may not merely state that the modification or combination would have been obvious to one of ordinary skill in the art without pointing out in the prior art a suggestion of the desirability of the proposed modification.

The Examiner did not provide a proper motivation to combine the different elements from *Bendinelli* and *Pfieffer*. The Examiner states that it would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of *Pfeiffer* with those of *Bendinelli* and add the use of DTD files with XML files to increase organization and allow for validation of an XML file. However, the motivation for the combination of *Bendinelli* and *Pfeiffer* is not based on any rationale, suggestion or motivation provided by the references. *Bendinelli* merely teaches providing program code containing a configuration for a VPN on a disk, wherein the program code may be in the form of XML. There is no teaching or suggestion for establishing a security policy format as a DTD file in any section of either *Bendinelli* or *Pfeiffer*. Thus, the Examiner is merely stating that the references could have been combined without offering any suggestion for the combination of the references.

**E. Even if the references could be combined, the combination would not form the presently claimed invention.**

Even if the references could be properly combined, the combination of the references would not form the presently claimed invention. The present invention is directed towards establishing a security policy specification format as a DTD file for automatically configuring IP security tunnels. A combination of *Bendinelli* and *Pfieffer* would not form the presently claimed invention in claim 2. Instead, a combination of the references would merely result in an XML document containing program code and information for a VPN and a DTD file that determines the validity of the XML file. Thus, any alleged combination of *Bendinelli* and Pfeiffer is not sufficient to form the claimed invention as recited in claims 2-4, 15-17, and 28-30.

**F. The claimed invention may only be reached through an improper use of the disclosed invention as a template to piece together and modify the prior art.**

Moreover, the Examiner may not use the claimed invention as an "instruction manual" or "template" to piece together the teachings of the prior art so that the invention is rendered

obvious. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Such reliance is an impermissible use of hindsight with the benefit of applicant's disclosure. *Id.* Therefore, absent some teaching, suggestion, or incentive in the prior art, *Bendinelli* and *Pfieffer* cannot be properly combined to form the claimed invention. As a result, absent any teaching, suggestion, or incentive from the prior art to make the proposed combination, the presently claimed invention can be reached only through the impermissible use of hindsight with the benefit of applicant's disclosure as a model for the needed changes.

Dependent claims 15 and 28 recite subject matter addressed above with regard to claim 2 and are allowable at least under the same rationale. At least by virtue of their dependency on claims 2, 15, and 28, dependent claims 3-4, 16-17, and 29-30 are patentable over any alleged combination of *Bendinelli* and Pfeiffer for the same reasons set forth above with respect to claims 2, 15, and 28.

Therefore, the rejection of claims 2-4, 15-17 and 28-30 under 35 U.S.C. § 103(a) has been overcome.

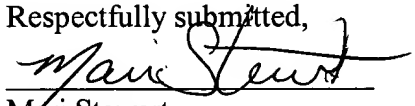
## V. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: November 14, 2005

Respectfully submitted,



Mari Stewart
Reg. No. 50,359
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants